Claims:

1. An apparatus comprising:

Management Frames utilized in wireless communications associated with said apparatus; and

said Management Frames being protection-capable or non-protection-capable and wherein said Management Frames indicate whether or not they are protection-capable.

2. The apparatus of claim 1, wherein at least one of said Management Frames is an Action Frame.

3. The apparatus of claim 2, wherein said wireless communications further comprises a Robust Security Network (RSN) Capabilities bit to be added for Action Frame protection negotiation.

4. The apparatus of claim 3, wherein said Action Frame protection negotiation is provided by a Beacon/Probe Response source setting said RSN bit to indicate that protection is required for all protection-capable Action Frames.

5. The apparatus of claim 3, wherein if said RSN Capabilities bit is set to protection-capable, said Action Frames may be protected by applying the IEEE

802.11i CCMP protocol construction to said protection-capable Action Frames.

6. The apparatus of claim 3, wherein if said RSN Capabilities bit is set to protection-capable, said Action Frames may be protected by applying the IEEE 802.11i TKIP protocol construction to said protection-capable Action Frames.

7. The apparatus of claim 5, wherein said CCMP protocol uses CCM to encrypt the Management Frame payload and to protect selected Management Frame header fields from modification.

8. The apparatus of claim 5, wherein said apparatus is a pair of wireless stations (STA).

9 The apparatus of claim 8, wherein at least one of said pair of wireless stations (STA) is an access point (AP).

10. The apparatus of claim 6, wherein said TKIP protocol uses RC4 to encrypt the Management Frame payload and uses Michael to protect selected Management Frame header fields from modification.

11. The apparatus of claim 6, wherein said apparatus is a pair of wireless stations (STA).

12 The apparatus of claim 11, wherein at least one of said wireless stations (STA) is an access point (AP).

13. The apparatus of claim 8, wherein said STA sourcing Beacons and Probe Responses sets to 0 if said protected Action Frames are not supported/enabled; said STA sets to 1 if said protected Action Frames supported and enabled; said responding STA sets to 0 if it doesn't support protected Action Frames; and said responding STA sets to the value set by said sourcing STA if it supports protected Action Frames.

14. The apparatus of claim 1, wherein said wireless communications is an 802.11 wireless LAN.

15. A method of protecting Management Frames in wireless communications, comprising:

establishing said Management Frames as protection-capable or non-protection-capable; and

protecting said Management Frames if said Management Frames are protection-capable.

16. The method of claim 15, wherein said step of protecting said Management Frames, comprises:

adding a Robust Security Network (RSN) Capabilities bit to said Management Frames for Management Frame protection negotiation, wherein if said RSN Capabilities bit is set to protection-capable, said Management Frames may be protected by applying a protection protocol to said protection-capable Management Frames.

17. The method of claim 16, wherein said Management Frame protection negotiation is provided by a Beacon/Probe Response source setting said RSN bit to indicate that protection is required for all protection-capable Action Frames.

18. The method of claim 16, wherein said protection protocol is the IEEE 802.11i CCMP protocol construction.

19. The method of claim 15, wherein at least one of said Management Frames is an Action Frame.

20. The method of claim 16, wherein if said RSN Capabilities bit is set to protection-capable, said Management Frames may be protected by applying the IEEE 802.11i TKIP protocol construction to said protection-capable Action Frames.

21. The method of claim 18, wherein said CCMP protocol uses CCM to encrypt the Management Frame payload and to protect selected Management

Frame header fields from modification.

22 The method of claim 20, wherein said TKIP protocol uses RC4 to encrypt the Management Frame payload and uses Michael to protect selected Management Frame header fields from modification.

23. The method of claim 15, wherein said wireless communications is wireless communications between a pair of wireless stations (STA), one which might be an access point (AP).

24. The method of claim 23, wherein said sourcing STA sets to 0 if said protected Management Frames are not supported/enabled; said sourcing STA sets to 1 if said protected Management Frames are supported and enabled; said STA sets to 0 if it doesn't support protected Management Frames; and said STA sets to value set by said AP if it supports protected Action Frames.

25. The method of claim 15, wherein said wireless communications is an 802.11 wireless LAN.

26. An article comprising a storage medium having stored thereon instructions, that, when executed by a computing platform, establishes, in a wireless communication environment, protection-capable and non-protection-

capable Management Frames, said protection-capable Management Frames being protected.

27. The article of claim 26 wherein said protection-capable Management Frames being protected are protected by adding a Robust Security Network (RSN) Capabilities bit to said Management Frames for Management Frame protection negotiation, wherein if said RSN Capabilities bit is set to protection-capable, said Management Frames may be protected by applying a protection protocol to said protection-capable Management Frames.

28. The article of claim 27, wherein said Management Frame protection negotiation is provided by a Beacon/Probe Response source setting said RSN bit to indicate that protection is required for all protection-capable Action Frames.

29. The article of claim 27, wherein said protection protocol is the IEEE 802.11i CCMP or TKIP protocol construction.

30. The article of claim 26, wherein at least one of said Management Frames is an Action Frame.

31. The article of claim 29, wherein said CCMP protocol uses CCM to encrypt the Management Frame payload and to protect selected Management

Frame header fields from modification, or uses the TKIP protocol which uses RC4 to encrypt the Management Frame payload and Michael to protect selected Management Frame header fields from modification.

32. The article of claim 26, wherein said wireless communications is 802.11 wireless communications between a pair wireless stations (STA), one of which may be an access point (AP).

33. A system to protect Action Frames in Wireless LAN Communications, comprising:

a first wireless station (STA); and

a second STA in communication with said first STA, said communication includes non-protection-capable Action Frames and protection-capable Action Frames.

34. The system of claim 33, wherein if it is desired not to protect Action Frames, then STAs shall send all Action Frames without protection, including all protection-capable Action Frames.

35. The system of claim 33, wherein if it is desired to protect Action Frames, then a STA shall protect all protection-capable Action Frames, said protection provided by adding a Robust Security Network (RSN) Capabilities bit to

said Action Frames for Action Frame protection negotiation, wherein if said RSN Capabilities bit is set to protection-capable, said Management Frames may be protected by applying a CCMP protocol which uses CCM to encrypt the Management Frame payload and to protect selected Management Frame header fields from modification, or by applying the TKIP protocol which uses RC4 to encrypt the Management Frame payload and Michael to protect selected Management Frame header fields from modification.

36. The system of claim 33, where said first STA shall not send protection-capable Action Frames at all if said second STA has not agreed to protection.

37. The system of claim 33, if the wireless communication requires protected Action Frames, then said first or said second STA shall discard any unprotected protection-capable Action Frame it receives.

38. The system of claim 37, wherein the discard of any unprotected protection-capable Action Frames includes those received before an IEEE 802.11i 4-Way Handshake completes.

39. The system of claim 33, wherein neither said first or said second STA shall attempt to protect non-protection-capable Action Frames it sends and shall

discard any it receives protected.

40. The system of claim 33, further comprising a STA in communication with said second STA.